CASE NO. 5:23-cv-607

EXHIBIT B

Appendix II: What Can Consumers Do After a Data Breach?

Figure 3 below provides information on actions consumers can take to monitor for identity theft or other forms of fraud, protect their personal information, and respond if they have been a victim of identity theft. This information summarizes prior GAO work and comments of academic, consumer organization, industry, and government experts.[1]

[1]GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, GAO-17-254 (Washington, D.C.: Mar. 30, 2017).

Figure 3: What Can Consumers Do After a Data Breach?

Prevent Fraud on New Credit Accounts

Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Place a credit freeze** on credit reports at Equifax, Experian, and TransUnion—the three nationwide consumer reporting agencies.	• Prevents identity thieves from opening new credit accounts in an individual's name—where credit reports are required. • Guardians can place credit freezes for minor children (under age 16) or adults who are incapacitated.	• Consumers must request a freeze at each of the three agencies separately. • Could still cause delays in approval of loans or other credit applications, especially if consumer forgets or loses the personal information number (PIN) the agencies give to consumers to unfreeze their credit reports. • Freezes do not prevent fraud on existing accounts (for example, the use of a stolen credit card number to make charges on a credit card). • Freezes do not prevent other types of harm, such as tax refund or medical identity fraud. • Not all access to credit reports is frozen (for example, still allowed for insurance underwriting and employment background checks). • Credit reports at agencies other than Equifax, Experian, and TransUnion will not be frozen (for example, those used to open utility accounts).
 **Place a fraud alert** at the three nationwide consumer reporting agencies, which lasts 1 year and can be renewed.	• Fraud alerts let businesses know that a consumer may have been a victim of fraud. • Businesses must take extra steps to verify the identity of the individual seeking to open accounts. • Members of the military can place active duty alerts.	• Consumers can request a fraud alert at one of the three agencies and this agency must notify the other two to place the alert. • Victims of identity theft can place extended fraud alerts that last for 7 years. • Fraud alerts still allow access to credit reports. • Businesses that do not use the three agencies will not see the alert.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Monitor for Some Types of Fraud on Financial Accounts

Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Review free credit reports every 12 months** (from Equifax, Experian, and TransUnion) at annualcreditreport.com.	• Can help consumers spot suspicious activity or fraud involving credit accounts.	• Consumers can check one of the three reports every 4 months to improve chances of catching problems throughout the year.
 **Review bank and other financial account statements regularly or set up free automatic alerts.**	• Can alert consumers to suspicious activity on their accounts.	• The availability and features of alerts may vary among financial institutions.
 **Consider enrolling in credit or identity monitoring services.**	• Credit monitoring can alert consumers after the fact that someone may have used their personal information to open a credit account (take out a loan or sign up for a credit card). • Identity monitoring can alert consumers of misuse of personal information or appearance of their information on illicit websites (the “dark web”).	• These services do not directly address risks of medical identity theft, identity theft tax refund fraud, or government benefits fraud. • Credit monitoring can spot fraud but generally cannot prevent it, and does not identify fraud on existing or noncredit accounts. • Identity monitoring also cannot prevent fraud. • It is unclear what actions consumers can take once alerted that their information appears on the dark web other than continuing to monitor their accounts. • These services may be part of a package of identity theft services, including restoration services, or identity theft insurance. • Free services that entities that have experienced data breaches may offer to affected consumers vary in the type and level of service and may only last for 1-2 years. Risks can exist for much longer. • Paid services typically cost $5–$30 a month.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Monitor for Other Types of Identity Theft or Fraud

Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Mobile Phone or Utility Account Fraud**		
Review mobile phone and utility bills regularly.	• Can spot suspicious activity on existing accounts.	• Consumers with credit freezes may need to lift them before applying for new utility or phone accounts.
 **Medical Identity Theft**		
Review medical bills and health insurance explanations of benefits.	• Can spot suspicious activity, such as bills or insurance claims for services consumers did not receive.	• Consumers who spot problems can contact fraud departments at health insurers.
 **Identity Theft Tax Refund Fraud**		
File tax returns early.	• Provides less time for a fraudster to file in an individual's name.	• Consumers who experience identity theft tax refund fraud can file affidavits with the Internal Revenue Service (IRS) and through IdentityTheft.gov, and may be eligible to obtain an Identity Protection Personal Identification Number from IRS.
 **Government Benefits Fraud**		
Set up an online account at the Social Security Administration and check it regularly.	• Can spot suspicious activity, such as benefits redirected to another address.	• Other government benefits, such as unemployment insurance, also can be susceptible to identity fraud.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

How to Respond after Identity Theft		
Consumer Option	How This Option Can Help	Consumers Should Be Aware
Visit identityTheft.gov to set up an account, fill out, and file necessary reports.	• Helps users determine what steps to take depending on the type of information stolen or type of identity theft. • Can generate an Identity Theft Report that can be used to help contact consumer reporting agencies, law enforcement, and other entities. • Can generate an IRS Identity Theft Affidavit (IRS Form 14039) that can be submitted directly to IRS. • Provides information on what companies to contact and how to remove incorrect information.	• The Federal Trade Commission (FTC) also has a telephone help line and online chat feature.
Contact state or local government resources, such as consumer protection help lines or victim services offices.	• Some states and local governments can provide one-on-one assistance.	• States and localities vary in the services offered.
Consider using commercial identity restoration services.	• Can reduce consumer time and effort in dealing with the effects of identity theft, such as by interacting with creditors on the consumer's behalf.	• Service levels can vary significantly among companies. Some provide hands-on assistance, while others largely provide information. • May be included in a package of identity theft services, which may also include credit or identity monitoring or identity theft insurance. Paid services typically cost $5–$30 a month and free services may only be offered for 1-2 years.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230

Protect Personal Information in Other Ways

Consumer Option	How This Option Can Help	Consumers Should Be Aware
 **Adopt Good Practices for Online Accounts** • Protect passwords and do not re-use them. • Use two-factor authentication when offered (for example, entering a one-time code sent to a mobile phone when logging in to an online account). • Choose strong passwords and consider using a software application that helps manage passwords. • Do not click on links in emails or open attachments from unknown senders. • Remember that public WiFi may not be secure.	• Can prevent unauthorized access to online accounts and other data intrusions.	• While personal security practices are important, consumers have limited control over how private entities secure their data.
 **Protect social media accounts** by checking privacy settings, and consider limiting information shared.	• Restricts how much information is visible to strangers and their ability to misuse it.	• Privacy terms and conditions can change, so it is important to check settings periodically.
 **Do not provide personal information over the phone (or by email or text) unless you've initiated the call (or communication).**	• Prevents identity thieves from obtaining information that can be used to commit fraud.	• Consumers can do online searches to verify identities of requesters, or check with experts, before giving out information. • Consumers should not trust caller ID and should hang up on robocalls and report such calls to FTC at ftc.gov/complaint.
 **Shred documents and mail with Social Security numbers or other personal information.**	• Prevents identity thieves from finding sensitive information in trash.	• Consumers can contact the U.S. Postal Service if they believe their mail is being stolen or misdirected. • Consumers can opt out of receiving credit card and other offers in the mail at 1-888-5-OPT-OUT (1-888-567-8688) or www.optoutprescreen.com.

Sources: GAO analysis, Federal Trade Commission, Consumer Financial Protection Bureau, and consumer and industry organizations. | GAO-19-230